Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0519-V3-2021

for

ORGA 6141 online V3.8.0:1.2.0

from

Ingenico Healthcare GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0519-V3-2021 (*)

eHealth: Smart Card Readers

ORGA 6141 online
V3.8.0:1.2.0

from	Ingenico Healthcare GmbH
PP Conformance:	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017
Functionality:	PP conformant Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 22 March 2021

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Head of Division

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product ORGA 6141 online, V3.8.0:1.2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0519-V2-2018. Specific results from the evaluation process BSI-DSZ-CC-0519-V2-2018 were re-used.

The evaluation of the product ORGA 6141 online, V3.8.0:1.2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 March 2021. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Ingenico Healthcare GmbH.

The product was developed by: Ingenico Healthcare GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 22 March 2021 is valid until 21 March 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product ORGA 6141 online, V3.8.0:1.2.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Ingenico Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the smart card terminal ORGA 6141 online Version 3.8.0:1.2.0 which fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system.

It has a card terminal with two ID1 Slots (HPC and eGK) and two SMC Slots (SM-KT (supporting SMC-B and SMC-KT cards), a 20 key keypad, USB and LAN interfaces for the use in the German healthcare system with KVK, HPC and eGK generation 1+ and generation 2. Connection to a connector/SAC is possible via LAN and TCP/IP-protocol.

In its core functionality the TOE is not different from any other smart card terminal which provides an interface to one or more smart cards including a mean to securely enter a PIN.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF_1: Trusted Communication Channels	All communication channels used by the eHealth/SAC applications to the connector/SAC and remote users are trusted communication channels.
SF_2: Identification & Authentication	The TOE provides several authentication mechanisms for the administrator and other users.
SF_3: Network Connections	The TOE accepts different subsets of SICCT commands depending on the pairing and valid certificates.
SF_4: Secure Update	The TOE only allows firmware updates after verification of the integrity and authenticity of that firmware.
SF_5: Secure PIN-entry	No subject shall read out the PIN or management credentials. All PINs are stored in volatile memory only.
SF_6: Secure Data Deletion	All PINs, cryptographic keys and all information that is by a card in a slot of the TOE or by the connector/SAC will be overwritten with 0x00 when they are no longer used.
SF_7: Secure Management-Functions	The TOE is aware of three roles: administrator, reset administrator and user. The secure management functions are only available to the TOE administrator after successful identification and authentication.
SF_8: Self-Test	The TOE can perform self-test on power-on and after activation by an authorized user.
SF_9: Secure Fail-State	The TOE will be put in a secure state in the case of:

TOE Security Functionality	Addressed issue
	● an alarm condition indicates possible tampering, or ● self-test detects an error, or failure during firmware update.
SF_10: Physical Protection of the TOE	The TOE is protected against unnoticed tampering by security seals. The TOE has an alarm function constantly checking for opening the TOE housing and a drill and probing protection foil.
SM_1: Sealing	The TOE is protected against unnoticed manipulations by security seals.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3, 3.4 and 3.5.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

ORGA 6141 online, V3.8.0:1.2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	TOE hardware part.	HC 03000000010301 or HC 03000000020301	TOE hardware part.
2	FW	Firmware Image	3.8.0:1.2.0	Initially included in the TOE.
3	DOC	User guide (Bedienungsanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0) [11] With the hash value (SHA256): 77eb3721fee4ec3c88a58232c2efea4d4a9d53d3059f2d0d305fb24e8aff6cae	21.1.1	Provided by the developer on their homepage.
4	DOC	Brief instruction (Kurzanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0) [12]	20.2.1	Delivered with the delivery package of the TOE.

No	Type	Identifier	Release	Form of Delivery
5	DOC	Endnutzer-Checkliste „Sichere Lieferkette“ [13]	20.7.1	Provided by the developer on their homepage.

Table 2: Deliverables of the TOE

The TOE is delivered to the end user in such a way as defined by the secure delivery chain [13].

According to [13], the TOE will be firstly delivered from developer Ingenico Healthcare GmbH to the company CGM (CompuGroup Medical Deutschland AG). From this point the secure delivery chain is identical to the certified secure delivery chain (Cert.-ID.: BSI-DSZ-CC-0950).

The transport to the user is also defined in the concept of the secure delivery chain (BSI-DSZ-CC-0950). The service technician or the end user installs the product **ORGA 6141 online** within the premises of the end user. The guidance defines all steps the end user has to perform to check if the secure delivery chain was correctly used and to check that the TOE is not manipulated or replaced and therefore the integrity and authenticity of the TOE is guaranteed.

The TOE can be identified within the management menu as following: Services → Status → TOE identification:

- Softwareversion 3.8.0, Hardware-Version 1.2.0
- Produktversion 3.8.0:1.2.0

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- TOE Access, and
- Trusted Path/Channels.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.ENV: It is assumed that the TOE is used in a controlled environment,

- OE.ADMIN: The administrator of the TOE and the medical supplier shall be non- hostile, well trained and have to know the existing guidance documentation of the TOE,
- OE.CONNECTOR: The connector in the environment has to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a means for mutual authentication
- OE.SM: The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate,
- OE.PUSH_SERVER:The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates and
- OE.ID000_CARDS: All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE.

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

A high level description of the IT product and its major components can be found in the Security Target [6], chapter 1.3.1 + 1.3.2.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Developer's Test according to ATE_FUN

TOE test configurations:

The Security Target [6] has identified solely one configuration of the TOE under evaluation. Nevertheless, the developer used three TOE test configurations for his testing approach:

- C1: TOE without any modification. The setup comprises the TOE connected to a computer via LAN.
- C2: TOE with debug capabilities. The TOE offers serial access to the system. Similar to C1 this TOE is also connected to a computer via LAN.
- C3: TOE modified for hardware tamper protection tests. This TOE uses the same firmware source code as C1 but has some debugging options enabled that allow triggering the tamper protection without erasing the master key.

TOE test environment:

The test setup comprises a laptop, a Connector, a TOE and three virtual card kits. Further hardware is used to create a LAN, to connect all used components.

Testing approach:

- Coverage and depth tests are done together.
- The tests considered the different roles that can access the TOE.
- The tests covered all TSF subsystems in the TOE design.
- The developer provided mappings to the tested TSFI(s), SFR(s), subsystem(s), and use cases.
- Different testing approaches were used:
  - Code analysis, and
  - Test suite (automatic and manual test).
- The test descriptions comprise (inter alia):
  - Pre conditions: Preparative steps
  - Test steps: Core test steps
  - Post conditions: Clearance steps to tidy up before the next test.

Verdict for the activity:

The developer's testing efforts have been proven sufficient to demonstrate that the TSFIs and subsystems perform as expected.

All test cases in each test scenario were run successfully on the TOE and they all passed according to their expected result.

7.2. Evaluator Tests

For this re-evaluation a subset of tests from the base evaluation was repeated.

TOE test configurations:

The evaluation body used the same test configurations and test environment as the developer during functional testing.

TSFI selection criteria:

The evaluation body chose to broadly cover the existing interfaces without specific restrictions.

All interfaces were considered during testing.

Developer tests repeated:

The evaluation body chose to inspect all developer tests. They also chose to repeat all tests but in the end six tests were not repeated due to their complexity.

Verdict for the sub-activity:

No deviations were found between the expected and the actual test results.

7.3. Penetration Testing according to AVA_VAN

Overview:

The configuration defined in the ST was tested. Furthermore, different TOE variants were used during penetration testing to verify different mechanisms. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Moderate was actually successful.

Penetration testing approach:

The evaluation body conducted penetration testing based on functional areas of concern (according to CEM §1549) derived from SFRs and architectural mechanisms. The areas were prioritized with regard to various factors, e.g. attack surface, estimated flaw likelihood, developer testing coverage, detectability of flaws during developer testing. Medium and high areas were guaranteed to be penetration tested, with a stronger emphasis on high priorities. Low priorities were also considered during penetration, but could be less emphasized, if developer tests were found to be sufficient. The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluators chose the analytical approach. Combined approaches were also applied.

TOE test configurations:

The TOE was delivered by the developer in different configurations: This includes a final operational, a special ATE variant and a special AVA variant. The ATE configuration is only used for self-protection tests. It allows the evaluator to safely trigger various tamper protection circuits, that otherwise would destroy the TOE. The AVA configuration is equipped with a serial connection. This allows the evaluator to have a look at the running system and, for example, review the list of running processes. Both variant are using modified hardware and software. The software is modified using compile time switched. Beside that, the source code for all three versions is the same.

Attack scenarios having been tested:

The evaluation body considered penetration testing in the following areas (according to CEM §1549):

- TLS Connections,
- Update,
- Hardening Mechanisms,
- Self-Protection, and
- Network Services.

Tested security functionality:

The evaluator ensured that all areas listed above are tested. Actually, the evaluation body used a more detailed list during the analysis and testing. The penetration testing was then conducted based on priorities as described above. Therefore, a complete coverage of security functional testing based on technical areas of concern is performed.

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Moderate was actually successful in the TOE’s operational environment provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- TOE software version: 3.8.0

- TOE hardware version: 1.2.0

There is only one evaluated configuration of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 3 package including the class ASE as defined in the CC (see also part C of this report)
- The components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0519-V2-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on:

- The TOE and the related developer evidence were updated to Version 3.8.0:1.2.0.
- The hardware parts of the TOE are unchanged, but additional testing regarding the hardware of the TOE was performed.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

No.	Purpose	Cryptographic mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1.	TLS key establishment	Diffie-Hellman as part of TLS cipher suites TLS_DHE_RSA_	[RFC5246]	2048	[RFC3526], DH group = 14, DH min exponent length = 384	FCS_CKM.1.1/ Connector

No.	Purpose	Cryptographic mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA			bits, Forward secrecy = yes	
2.	TLS key establishment	Elliptic Curve Diffie-Hellman as part of TLS cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[RFC5246], [RFC5289], [RFC4492]	256, 384	According to [gemSpec_Krypt, A_17124 and 5.8] brainpoolP256r1 and brainpoolP384r1 elliptic curves must be supported, cf. [RFC5639] and [RFC7027]	FCS_CKM.1.1/ Connector
3.	TLS Peer Authentication	RSA-2048 as part of TLS cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC5246]	2048	Limited support for TLS v1.2, according to [gemSpec_Krypt]	FCS_CKM.1.1/ Connector
4.	TLS Peer Authentication	ECDSA as part of the TLS cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[RFC5246], [RFC5289], [RFC4492]	256	[gemSpec_Krypt, A_17090]	FCS_CKM.1.1/ Connector
5.	TLS payload encryption	AES-128 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA), AES-256 (TLS_DHE_RSA_WITH_AES_256_CBC_SHA) in CBC mode	[RFC5246]	128, 256	Limited support for TLS v1.2, according to [gemSpecKrypt]	FCS_CKM.1.1/ Connector
6.	TLS payload encryption and message authentication	AES-128, (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SH	[RFC5246], [RFC5289]	128, 256	[gemSpec_Krypt]	FCS_CKM.1.1/ Connector

No.	Purpose	Cryptographic mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		A256), AES-256 (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384) in GCM mode				
7.	TLS Message Authentication	HMAC-SHA as part of TLS cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC5246]	160	Limited support for TLS v1.2, according to [gemSpec_Krypt]	FCS_CKM.1.1/ Connector
8.	TLS Signature Verification	SHA-256 with RSA	[PKCS#1]	2048	[FIPS180-4]	FCS_CKM.1.1/ Connector
9.	TLS Signature Verification	SHA-256 with ECDSA	[RFC5246], [RFC5289], [RFC4492]	256	[gemSpec_Krypt, A_17090]	FCS_CKM.1.1/ Connector
10.	TSF Signature Verification	RSASSA-PKCS1-V1_5 with SHA-256	[PKCS#1]	2048	[FIPS180-4]	FCS_COP.1.1/ SIG
11.	TSF Signature Verification	RSASSA-PKCS1-V1_5 with SHA-256	[PKCS#1]	4096	[FIPS180-4]	FCS_COP.1/ SIG_TSP
12.	TSF Signature Verification	RSASSA-PKCS1-V1_5 with SHA-256	[PKCS#1]	4096	[FIPS180-4]	FCS_COP.1/ SIG_FW

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to the application standards in the table above, especially the standards issued by gematik, the algorithms are suitable for the intended purposes listed above. An explicit validity period is not given.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
ALC	Life-Cycle Support
ARC	Security Architecture
ASE	Security Target Evaluation
ATE	Tests
AVA	Vulnerability Assessment
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CT	Card Terminal
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DEL	Delivery
eGK	elektronische Gesundheitskarte
eHC	Electronic Health Card
EAL	Evaluation Assurance Level

ECDSA	Elliptic Curve Digital Signature Algorithm (DSA)
ETR	Evaluation Technical Report
FLR	Flaw remediation
FUN	Functional tests
HPC	Health Professional Card
IND	Independent testing
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVK	Krankenversichertenkarte
LAN	Local Area Network
OSP	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
RSA	Asymmetrical Cryptographie (Rivest, Shamir und Adleman)
SAC	Signature Application Component
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC	Security Module Card
SM-KT	Security Module Kartenterminal
ST	Security Target
TSF	TOE Security Functionality
TSFI	TSF Interfaces
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	Trust-Service Provider that issues connector/SAC certificates
USB	Universal Serial Bus
VAN	Vulnerability analysis

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0519-V3-2021, Version 4.1.11, 2021-01-26, Security Target for the Evaluation of the Product ORGA 6141 online, Ingenico Healthcare GmbH

[7] Evaluation Technical Report, Version 3, 2021-03-11, TÜViT, (confidential document)

[8] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

[9] Configuration list HW for the TOE, Version 2, 2021-03-09, Datensatz PDXpert ORGA_6141_online_V1_3.8.0_Freigegeben, (confidential document)

[10] Configuration list SW for the TOE, Version 3.8.0, 2020-03-04, SVN Log files: SVN_log_ORGA 6141_online.zip, (confidential document)

[11] Guidance documentation for the TOE, Version 21.1.1, 2021-01-26, Bedienungsanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0, Ingenico

[12] Guidance documentation for the TOE, Version 20.2.1, 2020-02-19, Kurzanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0, Ingenico

[13] Guidance documentation for the TOE, Version 20.7.1, 2020-07-24, Endnutzer-Checkliste „Sichere Lieferkette“, Ingenico

[14] Lebenszyklusunterstützung, Dr. Neuhaus, Version 2.2, 2020-08-24, Sagemcom

[15] Sichere Lieferkette - Lieferung an Endnutzer/LEI, Version 6, 2018-05-15, Ingenico

[16] Sichere Lieferkette - für den Palettenversand von Großmengen, Version 22, 2018-12-13, Ingenico

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report